

# BILL ANALYSIS

Analyst: Deborah Barrett  
Work Phone: 845-4301

Department, Board, Or Commission	Author	Bill Number
Franchise Tax Board	Jones	AB 779

## SUBJECT

State Agencies Notify California Resident & Office Of Privacy Protection Of Breach in Security Of Data/Required Information To Be Included In Notices

## SUMMARY

This bill would do the following:

- Prohibit certain state agencies from retaining payment related data, and
- Require that the Office of Privacy Protection (OPP) be provided a copy of the notice sent to California residents when a breach of security of a system containing personal information has occurred.

## PURPOSE OF BILL

According to the author's staff, the purpose of the bill is to improve the quality of the notices issued for a breach of security, to implement industry standards to safeguard sensitive data, including not collecting unnecessary data to begin with, and to provide an incentive to protect the data by providing a reimbursement mechanism if data is breached.

## EFFECTIVE/OPERATIVE DATE

This bill would be effective January 1, 2008, and operative for security breaches that occur on or after July 1, 2008.

## ANALYSIS

### FEDERAL/STATE LAW

Under federal law, financial institutions are prohibited from disclosing the nonpublic personal information of their customers to a nonaffiliated third party unless they have provided notice as specified that such information may be disclosed to the third party.

Current federal and state law provides that returns and tax information are confidential and may not be disclosed, unless specifically authorized by statute. Any Franchise Tax Board (FTB) employee or member responsible for the improper disclosure of federal or state tax information is subject to criminal prosecution or fines or both. Improper disclosure of federal tax information is punishable as a felony and improper disclosure of state tax information is punishable as a misdemeanor.

Brian Putler, FTB Contact Person (916) 845-6333 (Office)	Executive Officer Selvi Stanislaus	Date 7/12/07
---	---------------------------------------	-----------------

Current state law requires a state agency to notify a resident of California in the event their personal information has been acquired by an unauthorized person due to a breach of security of that agency's computer system. A "breach of the security of the system" is the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information; however, an employee or agent of an agency is authorized to acquire personal information to perform his or her work duties.

"Personal information" is defined as a person's first name or first initial and last name, in combination with one or more of the following data elements when either the name or the data elements are not encrypted:

- Social security number,
- Driver's license number or California Identification Card number,
- Account number, credit card number, or debit card number along with the required security code, access code, or password.

Personal information does not include information that is legally made available to the general public from federal, state, or local government records.

State law requires notification to be made in the most expedient time possible and without unreasonable delay. If the agency maintains computerized data, but does not own the data, the agency must notify the owner or licensee of the information of the breach immediately following discovery. State law requires notification to be made by either written, electronic, or substitute notice. Any agency that maintains its own notification procedures is considered to be in compliance. Persons must be notified in accordance with those procedures and those procedures must be consistent with the timing requirements of current law.

### THIS BILL

This bill would prohibit, with certain exceptions, a person, business, or state agency that sells goods or services to any resident of California and accepts as payment a credit card, debit card, or other payment device from storing payment related data, except as specified.

This bill would also prohibit the following:

- Storage of sensitive authentication data subsequent to authorization,
- Storage of any payment related data that is not needed for business purposes,
- Retention of the primary account number unless retained in a manner consistent with other provisions of the bill and in a form that is unreadable and unusable by unauthorized persons anywhere it is stored,
- Sending payment related data across any open public network unless the data is encrypted using strong cryptography and security, and
- Allowing access to payment related data by any individual whose job does not require that access.

The provisions of this bill are not applicable to financial institutions that are in compliance with federal regulations relating to disclosure of nonpublic information if subject to compliance oversight by a state or federal regulatory agency with respect to those regulations.

This bill would require agencies subject to the payment related data restrictions to notify the owners or licensees of the data if the system containing that data is breached by an unauthorized person. This bill would provide that if notice is required, the agency whose system was breached is liable to the owner or licensee of the information for the reimbursement of all reasonable and actual costs of providing notice to consumers regarding the breach of the security of the system. Reasonable and actual costs include, but are not limited to, the costs of card replacement resulting from the breach of the system. If an agency can demonstrate that it complies with the payment related data restrictions of this bill, the agency is excused from reimbursement liability.

This bill would require notice to the owners or licensees of the payment related data to comply with certain requirements and would specify the type of information to be included in the notice. If the owner or licensee of the information is the issuer of the credit or debit card or the payment device or maintains the account information from which the payment device orders payment, the owner or licensee would be required to provide the California resident the information specified by this bill.

A law enforcement agency may delay notice if it determines that notice will impede a criminal investigation. Notice in those circumstances would be made after a law enforcement agency determines that the notice would not impede a criminal investigation.

This bill would require that if substitute notice as authorized is provided, the OPP must also be notified.

The provisions of this bill are intended to be severable, would repeal duplicative sections, and would provide double jointing language to resolve chaptering issues with AB 1298.

The provisions of this bill would not apply to FTB because the majority of FTB's transactions with taxpayers are payments of tax obligations, rather than purchases of goods or services. In addition, because the bill would make the requirement to notify owners or licensees of data in the event of a security breach conditioned upon being subject to the retention of payment related data requirements, these requirements in the bill would not apply to FTB either.

## **PROGRAM BACKGROUND**

FTB maintains a data retention policy for personal information that includes return information, which in turn includes payment related data. Retention time-frames vary from no less than the minimum amount of time required by law to seven years from the later of the original due date of the income tax return or the date the original or an amended tax return was filed.

Additionally, FTB does not accept debit card payment transactions, unless the debit cards can be used interchangeably as credit cards. An alternative electronic payment option offered by the department is Web Pay. Web Pay is an online application that can be used to make electronic withdrawals from taxpayers' checking or savings accounts to pay their personal income taxes. The payment can be scheduled up to one year in advance. Credit card payments are accepted for tax payments, but are not currently available for use in the non-tax debt programs the department administers.

## LEGISLATIVE HISTORY

SB 1744 (Bowen, 2005/2006) proposed to require an agency that suffers a breach of the security of a system containing personal data to provide a credit monitoring service to the affected persons for up to one year, at no charge. This bill did not pass out of the Senate Business and Professions Committee.

SB 852 (Bowen, 2005/2006) proposed to expand notification of breaches of security requirements to include breaches of computerized data in any format. This bill failed passage out of the Assembly Business and Professions Committee.

SB 1279 (Bowen, 2003/2004) would have applied the notice requirements for computerized data that had been breached to security breaches for all types of data. This bill remained with the Assembly Business and Professions Committee.

AB 700 (Simitian, Stat. 2002, Ch. 1054) requires a state agency to notify residents of California in the event their personal information has been acquired by an unauthorized person due to a breach of security of that agency's computer system.

## OTHER STATES' INFORMATION

The laws of the states of *Florida*, *Illinois*, *Massachusetts*, *Michigan*, *Minnesota*, and *New York* were reviewed. These states were selected due to their similarities to California's economy, business entity types, and tax laws. All of these states accept payment by credit card and use intermediaries to assist in the processing of the transactions. *Minnesota* charges a convenience fee directly to the taxpayer, and then remits that fee to the service provider. The other states' arrangements parallel California's.

All of these states have statutes for the breach of systems containing personal information similar to California's statutes. Notice is required for residents whose information may have been compromised. In certain circumstances, *New York* and *Minnesota* require notification to credit bureaus or the state consumer protection agency.

## **FISCAL IMPACT**

Because the department is unable to predict when a breach of security may happen or how extensive that breach may be, the costs that would be incurred to reimburse an owner of data is unknown. Because the requirements for notification of owners of data do not apply to FTB as noted in the “This Bill” discussion, no additional costs are expected.

## **ECONOMIC IMPACT**

This bill would not impact state income tax revenues.

## **VOTES**

Assembly Floor – Ayes: 58, Noes: 2

Senate Floor – Ayes: 30, Noes: 6

Concurrence – Ayes: 73, Noes: 0

## **LEGISLATIVE STAFF CONTACT**

Deborah Barrett  
Franchise Tax Board  
(916) 8454301  
[Deborah.Barrett@ftb.ca.gov](mailto:Deborah.Barrett@ftb.ca.gov)

Brian Putler  
Franchise Tax Board  
(916) 845-6333  
[brian.putler@ftb.ca.gov](mailto:brian.putler@ftb.ca.gov)